2003

The USA Patriot ACT: The Devil is in the Details

Elizabeth Brandt

The USA Patriot Act: The Devil is in the Details

By Elizabeth Barker Brandt and Jack Van Valkenburgh

In the August 2003 issue of *The Advocate*, Assistant U.S. Attorney Terry Derden urged the state's lawyers to "look at the Act."[1] After all, as most lawyers know, "the devil is in the details." David Nevin, Scott McKay and Dean Arnold analyze the significant changes brought about by the USA Patriot Act ("USAPA") and other post 9/11 policy changes. In this article, we take the Assistant U.S. Attorney's admonition to heart and "look" in detail at some of the specific provisions of USAPA as they relate to the Foreign Intelligence Surveillance Act (FISA)[2] and to the expansion of non-FISA surveillance. Those who seek reassurance from a detailed analysis of the USAPA, however, will find cold comfort. Such an analysis only serves to underscore concerns that the Act authorizes serious violations of civil liberties.

1. Roving Wiretap Orders

Section 206 of the USAPA significantly expands the scope of "roving wiretap orders." In 1986, Congress amended the wiretapping provisions of Title III of the federal criminal code to permit roving wiretaps.[3] A "roving wiretap" is one in which the specific location of the wiretap is not set forth in the order granting authority to wiretap. Under the 1986 provisions, in order to get such a wiretap under Title III, the government had to demonstrate probable cause and that the target was purposefully changing phones to thwart government surveillance.[4] In addition, before wiretapping could begin, the government needed to demonstrate that the target was actually using the phone line or was "reasonably proximate" to the line that was to be tapped.[5] In 1998, the "intentionally thwarting" standard was relaxed so that the government had to show only that the target's conduct in changing phones was thwarting the wiretap.[6] However, the requirements of probable cause and "reasonably proximity" to the line were not changed. These provisions ensured that the government could not use a roving wiretap order as a fishing expedition, and they limited the possibility that the tap would invade the privacy of individuals who were not targets.

Section 206 of USAPA applies a loosened version of the Title III roving wiretap authority to FISA. The inclusion of the roving wiretap provision in FISA permits criminal investigators to obtain a FISA order without demonstrating the probable cause as required for a Title III wiretap.[7] The new provision does not require the government to demonstrate that the target's conduct by changing phones is thwarting the tap. Moreover, the FISA provision eliminates the requirement of Title III that the government demonstrate that the target of the tap has actually used the phone to be tapped or been in reasonable proximity to it.

By loosening the requirements for a Title III roving tap and allowing the Foreign Intelligence Surveillance Court ("FISC") to issue such orders without making a finding of probable cause, judicial oversight of such orders is diminished. Moreover, since the government does not have to demonstrate that the target is thwarting a traditional wiretap, it is possible to use the roving wiretap as a fishing expedition. Finally, the FISA roving taps have a much greater probability of invading the privacy invasions of completely unrelated individuals.

U.S. Senator Larry Craig, leading a bi-partisan group that includes Senator Dick Durbin (D IL) and U.S. Senator Michael Crapo, has recently introduced legislation in the Senate that would curtail roving wiretaps to situations where at least the identity of the target of the wiretap is known. Entitled the "SAFE Act,"[8] the proposed legislation also would only permit the wiretap to go forward when the presence of the target at the tapped facility is known by the government prior to conducting the tap.[9] U.S. Representatives Butch Otter and Mike Simpson expect to introduce similar legislation in the House of Representatives.[10]

2. Sneak and Peek Warrants

Section 213 of the USAPA amends Federal Rule of Criminal Procedure 41 to permit delayed notification of a search. Rule 41 previously required that if a search was conducted in the absence of the property owner, the government had to leave a copy of the warrant and notify the issuing court of its actions. The Ninth Circuit has held that notice is constitutionally required, but it has not held that contemporaneous notice is always constitutionally required.[11] Some courts have recognized exceptions to the contemporaneous notice requirement in limited contexts where notification would endanger the life or physical safety of an individual; result in flight from prosecution, destruction of evidence or intimidation of witnesses; or otherwise seriously impair the investigation or delay trial.[12] The wiretap cases and wiretap statutes are sui generis because delayed notice is unavoidable in such cases. However, with respect to physical searches, the courts have allowed delayed notice only in very limited contexts—where there is serious danger to life or evidence, and only with respect to serious crimes, and only on a case-by-case basis.

Section 213 threatens to regularize sneak and peek searches. It permits delayed notification in any case in which the government demonstrates one of the above factors "may" occur, regardless of whether the investigation involves terrorism or the gathering of foreign intelligence. Such delayed notification is permitted even where the government seizes electronic information so long as the court issuing the warrant determines that delayed notification is "reasonably necessary." Section 213 does not require that a court be notified of the delayed notification and does not place any outside limit on when notification must take place.

The proposed SAFE Act would permit delayed notification, but only where the government demonstrates that notice of the search "will" result in endangering the life or physical safety of an individual, flight from prosecution, destruction of evidence or intimidation of witnesses; or otherwise seriously impair the investigation or delay trial. Moreover, the SAFE Act would require that notice be provided within seven days of the search, but also provides for extensions of the delay.[13]

3. Trap and Trace Devices and Pen Registers

Section 214 of USAPA extends the FISA standards for trap and trace devices and pen registers ("pen/trap devices")[14] to investigations against targets who are not even agents of a foreign power. FISA formerly limited pen/trap devices to those installed on facilities used by foreign agents or individuals engaged in international terrorist or clandestine intelligence activities.[15] Now, in order to obtain an order for a FISA pen/trap device, law enforcement officials no longer have to show that the facility is being used by a foreign agent; instead they need only show that the device is likely to reveal information relevant to a foreign intelligence investigation.[16]

In addition to eliminating the requirement that FISA pen/trap device orders be directed at foreign agents, Section 214 also extends such orders beyond telephonic communications to electronic communications. In other words, where a FISA pen/trap device order would previously have been available only for a facility used by a foreign agent and only for telephonic communications, it can now be obtained against any target or facility and can include e-mail as well as telephone information.

USAPA not only expands the scope of pen/trap orders under FISA, it also expands existing non-FISA law regarding the use of such devices in criminal investigations. Section 216 permits roving law enforcement pen/trap device orders and expands the scope of existing law to include electronic and cellular telephone communications. Prior to USAPA, federal law allowed law enforcement officials to obtain orders to install pen/trap devices on telephone lines only upon certification that the information to be obtained was relevant to an ongoing criminal investigation. These orders had to be obtained in the jurisdiction in which the telephone was located.[17] Moreover, the statutory authority for such orders was limited to telephone "lines."[18]

Under the new provisions of USAPA, the order for a trap and trace device or a pen register does not need to be obtained in the jurisdiction in which the phone is located and the order can apply not only to telephonic communication but also to cellular telephones identified by their electronic serial number, internet user accounts or e-mail addresses, and IP (internet protocols) and similar computer addressing information. Moreover, the pen register or trap and trace order can be used to obtain routing, addressing and signaling information such as a list of URLs[19] accessed by a computer user. Finally the USAPA revisions make clear that the section is not limited to "devices" that must be "attached" but could include the use of a computer software routine to collect the information.[20]

Under section 214, investigators could obtain a pen/trap device order either from the FISC or from a district court from the location of the search. To get the order, the government only must certify that what they seek is either relevant to a foreign intelligence investigation or to a criminal investigation. The order could be served on an Internet service provider ("ISP") in Idaho and could require the ISP to run a computer software routine to track any web page visited by one of the ISP's customers.

At the federal level, the constitutionality of warrantless pen/trap devices was conditioned upon the sense that the communicative and informational value of phone numbers was minimal. In *Smith v. Maryland*,[21] the U.S. Supreme Court held that obtaining telephone numbers using a pen register was not a search requiring law enforcement to demonstrate probable cause based on that reasoning. The Supreme Court conclusion regarding pen/trap devices was not without controversy. The Supreme Courts of a number of states, including Idaho, reached differing conclusions and required state officials to obtain warrants based on probable cause for the installation of pen/trap devices.[22] The communicative value of Internet addressing information is significantly greater than telephone numbers. URLs are not simply a list of numbers reaching a phone that may be answered by a number of different people. Rather URLs often contain the name of the web site sponsor. Moreover, attached to that URL is relatively stable content. Any person who goes to www.aclu.org views the same information that any other person who goes to that site sees.

4. Business Records

Section 215 of USAPA expands previous FISA provisions regarding business records and makes them applicable even when the target is not an agent of a foreign power. FISA previously provided that, where the target of the investigation was the agent of a foreign power, senior FBI officials could apply for a court order in connection with a foreign intelligence investigation for access to the records of common carriers, public accommodations providers, physical storage operators, and vehicle rental agencies.[23] The USAPA substantially rewrites these provisions. Now assistant agents in charge of FBI field offices can apply for such orders. The order can extend to any tangible object held by anyone (including documents, computer discs, etc.). Items sought need not relate to an identified foreign agent as previously required by FISA. Rather law enforcement officials must only show that the items are sought in connection with an investigation relating to international terrorism or clandestine intelligence activities.[24]

Pursuant to this provision of USAPA, federal law enforcement officials can collect employment records, internet records, credit card information and library borrowing information, all without even suggesting that the owner of the records was involved with or suspected of any criminal activity or involvement in foreign intelligence. In fact, criminal investigators could seek a FISA business records order based solely on the certification to the FISC that the information sought is needed as part of an investigation of clandestine intelligence activities. Using this order, they could obtain library borrowing records, employment and student records, credit card information and medication information for any individual, whether that person is the target of the investigation or a foreign agent.

The proposed SAFE Act would limit the reach of FISA business records orders by requiring that the government demonstrate and the judge find that the records pertain to a foreign power or agent of a foreign power.[25]

5. Nationwide Search Warrants

Rule 41 of the Federal Rules of Criminal Procedure formerly required a search warrant to be issued by a court in the jurisdiction in which the property to be searched is located. Section 219 of the USAPA allows a judge in a case involving domestic or international terrorism to issue a search warrant that can be executed either inside or outside the district where the court is located. Section 220 amends federal law to permit such warrants to be executed nationwide.[26]

Idaho Representative Butch Otter has spoken out against the use of such nationwide search warrants.[27] In one presentation he raised the specter of a judge in Manhattan passing on a search warrant authorizing the search of property in Idaho. The warrant was based on the belief of New York law enforcement agents that an Idaho resident was a potential terrorist because he was photographed driving a pickup truck past the United States Courthouse in Moscow, Idaho with nitrogen fertilizer, diesel fuel and several large barrels in the truck bed.[28] What is legitimate agricultural activity in Idaho could take on significant weight in a terrorism investigation in New York.

Conclusion

We do not deny that terrorism has taken many innocent lives, both within and without the United States. Nor do we object to any "updating" of federal law to address new technologies and new threats to public safety.

We do, however, insist that the changes to the surveillance authority of federal law enforcement officials embodied in the USAPA are far-reaching and significant. The cumulative impact of the provisions is startling. Viewed together, the provisions attempt an "end-run" around the Fourth Amendment's probable cause requirements. Although federal judicial oversight is not eliminated, it is seriously undermined by provisions that do away with probable cause, move the authority to order searches to the FISC or to courts outside the area to be searched, and permit searches of undesignated locations. Rather than evaluating a warrant request based on a factual record establishing probable cause, the federal judge is reduced to the ministerial role of ensuring that the necessary certifications are included in a search request. By opening the procedures of the FISC to criminal investigators and providing for nationwide orders, USAPA permits even this ministerial function to take place either in secrecy or in a location far from the context of the search.

ELIZABETH R. BRANDT is a Professor at the University of Idaho College of Law. She is a member of the boards of the national American Civil Liberties Union (ACLU) and of the ACLU of Idaho. In addition to teaching and writing in the area of Family Law, she also often writes and speaks on civil liberties issues.

JACK VAN VALKENBURGH is an attorney and Executive Director of the ACLU of Idaho

Endnotes

1 Terry Derden, *One Year Under the Patriot Act: Has the Sky Fallen?*, The Advocate, August 2003 at 15. "The Act," of course, is the USA Patriot Act, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the United States Code)

2 Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801-11 (2000, 18 U.S.C. §§ 2511, 2518-19 (2000)). In addition to the amendments to FISA, there are a number of other controversial provisions of USAPA including a broadened definition of terrorism, USAPA § 802, and restrictive amendments to immigration laws USAPA tit. IV

3 18 U.S.C. § 2518(11)(2000)

4 18 U.S.C. § 2518(11)(b)(ii) (2000).

5 18 U.S.C. § 2518(11)(b)(iv) (2000).

6 *See* ACLU, *How the USA PATRIOT Act Limits Judicial Oversight of Telephone and Internet Surveillance* (Oct. 23, 2001), *available at* http://www.aclu.org/congress/l102301g.html, (last visited October 2, 2003) (describing the 1986 and 1998 amendments to Title III allowing roving wiretaps)

7 *See* discussion of FISA probable cause requirements in the article by Nevin, McKay and Arnold in this issue of *The Advocate*.

8 The Security and Freedom Ensured Act of 2003, S. 1709, 108th Cong. (1st Sess. 2003).

9 SAFE Act, § 2.

10 *See Idaho Delegation Sponsors Measure to Clarify Patriot Act*, available at http://www.gop.gov/Item-news.aspx?docId=588367 (last visited October 22, 2003)

11 *United States v. Pritus*, 800 F.2d 1451, 1453 (9th Cir. 1986). *But see United States v. Simmons*, 206 F.3d 392 (4th Cir. 2000).

12 *See* 18 U.S.C. § 2705 (2000) (permitting delayed notification for search involving electronic communications held in third party storage for more than 180 days).

13 SAFE ACT § 4.

14 These are devices traditionally installed on a telephone line that track the telephone numbers called from that line (pen register) and the numbers from which calls are made to that that line (trap and trace device).

15 50 U.S.C. § 1842(c)(3) (2000).

16 *Id. See* CHARLES DOYLE, LAW DIVISION, CONGRESSIONAL RESEARCH SERVICE, TERRORISM: SECTION BY SECTION ANALYSIS OF THE USA PATRIOT ACT, 14 (Dec. 10, 2001), *available at* http://fpc.state.gov/documents/organization/7952.pdf (last visited October 2, 2003).

17 18 U.S.C. § 3127(3) (2001). *See also* ELECTRONIC PRIVACY INFORMATION CENTER, ANALYSIS OF PROVISIONS OF THE PROPOSED ANTI-TERRORISM ACT OF 2001, *available at* www.epic.org/privacy/terrorism/ata_analysis.html (Sept. 24, 2001).

18 *Id.*

19 URLs or "uniform resource locators" contain web addressing information. For example www.law.uidaho.edu is the URL for the University of Idaho College of Law's web site.

20 *Supra* note 16 at 13.

21 442 U.S. 735 (1979)

22 State v. Thompson, 113 Idaho 466, 745 P.2d 1087 (1988). For other states, *see, e.g., People v. Spoklede*, 666 P.2d 135 (Colo. 1983); *State v. Gunwall*, 720 P.2d 808 (Wash. 1986)

23 50 U.S.C. §§ 1861-63 (2000).

24 DOYLE, CRS, *supra* note 16 at 11

25 SAFE Act § 4

26 18 U.S.C. § 2703 (2000)

27 *See Votes to Repeal Sneak and Peek Searches* July 23, 2003 on TalkLeft: The Politics of Crime, available at http://www.talkleft.com/archives/000766.html (last visited October 27, 2003).

28 Comments made at *The Patriot Act and Community Resolutions* (Panel Discussion with U.S. Cong. Butch Otter, R. Idaho, Idaho State Senator Gary Schroder, Idaho State Rep. Shirley Ringo and Prof. Elizabeth B. Brandt) Palouse Peace Coalition, August 26, 2003.